PKI Adoption Case Study (for the OASIS PKIA TC)

Australian legal sector

PKI Project Title	Digital credentials for lawyers
Organisation concerned	A professional body
Timeframe of implementation	TBD
Date went live	Not applicable
Case study author	Stephen Wilson
Contact details	swilson@lockstep.com.au

1. Business background

Please describe the organisation, its business or function, and the broad nature of its transactions and/or online services (one or two paragraphs)

A peak professional body responsible for maintaining a register of practising lawyers. The body is interested on behalf of its members in enabling the transformation of legal services from paper to online transactions.

2. Objectives for the PKI Project

In the context of the business background, please describe the organisation's objectives in implementing PKI. Was the organisation seeking any or all of: better efficiencies, better security, better compliance? Include a description of the target users and their environment (five to ten bullet points).

- This was a scoping study delivering a concept of operations but not yet live
- Long term vision is to create high fidelity, trustworthy digital credentials equivalent to the traditional practising certificates issued to lawyers.
- Build infrastructure to support the use of digital certificates in signing routine online transactions undertaken by lawyers
- Generate major cost savings, time improvements, and workflow efficiencies as a result of eliminating paperwork from legal transactions
- Target "electronic conveyancing" of realty transactions as likely having highest business benefit impact

3. System notes

Please summarise relevant technical aspects of the systems and the PKI implementation, such as operating systems, client and server platforms, whether certificate production was insourced or outsourced, the types of key media and so on; ideally, please name the PKI vendors, though we appreciate that this is not always possible (five to ten bullet points).

- Client systems typical of office automation generally – mixture of Windows, Mac etc.

- Electronic conveyancing and other special applications for lawyers still under development, not possible to characterise at this stage
- Unusual feature is the distinct need for multiple digital signatures on transactions; may lead to unorthodox if not non-standard implementations
- Special XML variants … not yet fully reconciled with XMLsignatures
- PKI certificate production expected to be outsourced, with RA delegated to professional body's membership branches.

Please describe the application that was PKI-enabled, who was responsible for any modifications, including the relative efforts that went into developing new code versus off-the-shelf procurement (one paragraph).

No apps yet finalised.

See below brief discussion of electronic conveyancing and online court documentation, as future apps.

4. Business impacts

Describe the impacts the PKI project had on the organisation, both positive and negative; where possible try to quantify the benefits; try to distinguish between immediate impacts and "strategic", long term and/or indirect impacts (two or three paragraphs).

At the time of writing, this PKI project was incomplete.

5. Next steps and suggested improvements

What if any are the organisation's next steps in PKI? What would you do differently if you were starting all over again? What suggestions would you offer to others implementing PKI? (one or two paragraphs)

Next steps are to substantiate the return on investment (benefit = going paperless in select transactions; cost = hurdle cost of developing & implementing policies, RA, PKI service delivery etc.).

In the legal sector, there is some further thinking and analysis needed as to which online applications really merit digital signatures, and better definition of the role in which people act when they sign legal documents.

In Australia, electronic conveyancing (of real property transactions) is perhaps the most compelling application, as it involves high levels of risk, multiple parties, and has enormous potential benefits through better timeliness of closing transactions on line compared with face-to-face, and great paper related cost savings.

At the same time, the transformation of court documentation from paper to online would seem to represent a new demand for PKI. The integrity of court documentation, and in particular its resistance to deliberate tampering, should create a strong case for digital signatures.

As court information systems tend to be based on complex, large, expensive monolithic software applications, there probably needs to be strategic discussions at management level between vendors, the legal profession, and CAs, to forge a shared vision and give these innovations the appropriate priority to make the corresponding investment of R&D time and money happen.

6. Your suggestions to the PKI industry

Based on your experience, what would you like to see done in the PKI industry to facilitate adoption? (three to eight bullet points).

- Develop more up-to-date shared understanding of digital credentials, breaking the old mould of personal identity certificates which continues to confuse people
- Work on lower start up cost operational models and services, so that small communities of interest like professional societies can obtain certificates more easily
- Simplify Certificate Policy frameworks and templates, so that meaningful digital credentials can be provisioned without enormous and highly technical (actually arcane) effort devoted to CP/CPS development.